DISTRICT OF COLUMBIA RETIREMENT BOARD
Position Vacancy Announcement

ANNOUNCEMENT NO: **20130411**	POSITION: **Security Administrator**
OPENING DATE: April 11, 2013	CLOSING DATE: **Open until filled**
TOUR OF DUTY: 8:30 a.m.-5:00 p.m., Monday-Friday This position will also be on-call for three (3) days per month.	STARTING RANGE: **$74,800 - $93,500 DOQ (Grade 9)** **(Career Service) Entire Range: $74,800 - $115,566**
LOCATION: 900 7th Street, NW, 2nd Floor Washington, DC 20001	AREA OF CONSIDERATION: Open to all applicants
NUMBER OF VACANCIES: One (1)	TYPE OF APPOINTMENT: Probationary to Regular

This position is **NOT** in a collective bargaining unit.

*** ***Successful pre-employment criminal, financial, educational and certification background check required*** ***

ABOUT THE D.C. RETIREMENT BOARD: The District of Columbia Retirement Board is an independent agency of the District of Columbia Government. Our mission is to manage and control the assets of the D.C. Police Officers' and Firefighters' Retirement Plan and the D.C. Teachers' Retirement Plans as well as to administer benefits for the members of the plans.

POSITION SUMMARY

Under the general direction of the Director of Information Technology, the Security Administrator will ensure the secure operation of the agency's information systems and services including servers, network connections, storage devices, appliances, PCs, mobile devices, applications, databases, and data transfer devices and technologies. This includes designing the agency's data loss protection (DLP) policies and procedures, checking server and firewall logs, scrutinizing network traffic, establishing and updating virus scans, and troubleshooting. This person will also analyze and resolve security breaches and vulnerability issues in a timely and accurate fashion, and conduct user and system activity audits and conduct penetration testing where required.

PRIMARY RESPONSIBILITIES

1. Develop, implement, maintain, and oversee enforcement of policies, procedures and associated plans for system security administration and user system access based on industry-standard best practices.

2. Participate in the processes to obtain ISO 20000 certification for the agency, meet FIPS-140-2, FIPS-199, NIST-800-53, and moderate secure environment compliance.

3. Design, implement, and maintain cyber security strategies for the agency to minimize the risks of security breaches.

4. Participate in the design and implementation of disaster recovery plans and strategies for the agency with a goal of fault tolerance and disaster avoidance, to include telephone and telecommunications services, operating systems, databases, networks, servers, and software applications.

5. Assess need for any security reconfigurations (minor or significant) and execute them if required.

6. Conduct research on emerging products, services, protocols, and standards in support of security enhancement and development efforts.

7. Recommend, schedule, and perform security improvements, upgrades, and/or purchases.

8. Deploy, manage and maintain all security systems and their corresponding or associated software, including firewalls, intrusion detection systems, cryptography systems, and anti-virus software.

9. Manage connection security for local area networks, agency websites both internal and external, and e-mail communications.

10. Manage and ensure the security of databases and data transferred both internally and externally, and data maintained on agency devices.

11. Design, perform, and/or oversee penetration testing of all systems in order to identify system vulnerabilities.

12. Design, implement, and report on security system and end user activity audits.

13. Monitor server logs, firewall logs, intrusion detection logs, and network traffic for unusual or suspicious activity. Interpret activity and make recommendations for resolution.

14. Recommend, schedule (where appropriate), and apply fixes, security patches, disaster recovery procedures, and any other measures required in the event of a security breach.

15. Download and test new security software and/or technologies.

16. Perform system backups.

17. Administer and maintain end user accounts, permissions, and access rights to PCs, systems, appliances, and devices. Provide on-call security support to end-users.

18. Manage security and access control to the agency's computer facilities including headquarters and datacenter locations.

19. Other duties as assigned.

KNOWLEDGE, SKILLS AND ABILITIES

- Broad hands-on knowledge of firewalls, intrusion detection systems, anti-virus software, data encryption, and other industry-standard techniques and practices.

- In-depth technical knowledge of network, PC, and platform operating systems, including Cisco, Microsoft, and VMware products.

- Working technical knowledge of current systems software, protocols, and standards.

- Strong knowledge of TCP/IP and network administration/protocols.

- Hands-on experience with devices such as hubs, switches, and routers.

- Advanced knowledge of applicable practices and laws relating to data privacy and protection.

- Knowledge of federal security standards such as FIPS-199, FIPS-140-2, and NIST-800-53.

- Ability to interact and negotiate with vendors, outsourcers, and contractors to obtain protection services and products.

- Ability to adapt and work effectively in a government environment.

- Ability to develop and execute security strategies and establish and maintain systems of tracking performance against goals and expectations.
- Excellent written and verbal communication skills.
- Working knowledge of MS Office.

BEHAVIORAL COMPETENCIES

- Ability to work with significant level of independence and autonomy.
- Ability to work well under minimal supervision.
- Strong analytical and problem-solving skills to enable effective security incident and problem resolution.
- Proven ability to work under stress in emergencies, with the flexibility to handle multiple high-pressure situations simultaneously.
- Strong team-oriented interpersonal skills, with the ability to interface effectively with a broad range of people and roles, including vendors and IT-business personnel.
- Strong customer/client focus, with the ability to manage expectations appropriately, provides a superior customer/client experience and builds long-term relationships.
- Ability to influence others and demonstrate project leadership by working producing work in a timely and cost effective manner.
- Ability to maintain confidentiality of records and information.
- Stays abreast of concepts and trends through attendance at meetings, seminars, conferences, etc. Informs supervisor of new developments/trends.

QUALIFICATIONS

- Minimum of seven years' experience in the field of information technology and security administration.
- Bachelor's Degree in computer science or closely related field.
- Certifications in security, networking, and infrastructure management such as CISSP, Security+, SSCP, GSEC, ISECP, ITIL, MCSE, and CCNP are a plus.

WORKING CONDITIONS

- Normal office environment
- This position will be on-call for three (3) days per month.

COMPENSATION LEVEL: Grade 9

This job description indicates the general nature and level of work being performed by employees in this job. It is not intended to be an exhaustive list of all tasks, duties, and qualifications of employees assigned to this job. Incumbents may be asked to perform other duties as required.

HOW TO APPLY: Applicants must submit a completed DC2000 Employment Application, letter of interest discussing eligibility and qualifications, and resume.

The DC2000 Employment Application is available at http://www.dchr.dc.gov/ under "Forms and Applications" in the Information section.

Applicants claiming Veterans Preference must submit official proof with application.

All educational and experience requirements used to determine eligibility for this position must be officially verified at the time of appointment. No offer of employment will be deemed fulfilled without such verification(s).

WHERE TO APPLY: **Submit application materials to:** **HR Director**
DC Retirement Board
900 7th Street NW, 2nd floor
Washington, DC 20001

Or fax materials to: **(202) 566-5000**
Attention: HR Director

Or e-mail materials to: dcrb.vacancies@dc.gov

NOTE: It is imperative that all information on the DC2000, resume and supporting documents be both accurate and truthful and is subject to verification. Misrepresentations of any kind may be grounds for disqualification for this position or termination.

NOTICE OF NON-DISCRIMINATION: In accordance with the DC Human Rights Act of 1977, as amended, DC Official Code, §2-1401.01, et seq. (Act), the District of Columbia Public Schools does not discriminate in its programs and activities on the basis of actual or perceived race, color, religion, national origin, sex, age, marital status, personal appearance, sexual orientation, family status, family responsibilities, matriculation, political affiliation, disability, source of income or place of residence or business. Sexual harassment is a form of sex discrimination, which is prohibited by the Act. In addition, harassment based on any of the above protected categories is prohibited by the Act. Discrimination in violation of the Act will not be tolerated. Violators will be subject to disciplinary action.

NOTICE OF BACKGROUND INVESTIGATION AND PENALTIES FOR FALSE STATEMENTS: An offer of employment with the DCRB is contingent upon the completion and satisfactory result of a criminal, education and financial background investigation conducted by the DCRB or authorized agent prior to commencement of duty. In addition, an offer of employment for a position with specified education and certification qualification requirement(s) is contingent upon the completion and satisfactory result of an educational and/or certification background investigation conducted by the DCRB or authorized agent prior to commencement of duty (Pursuant to DCRB Policy No. DCRB-09-1-01).

Applicant understands that a false statement on any part of your application, including materials submitted with the application, may be grounds for not hiring you, or for firing you after you begin work (D.C. Official Code, section 1-616.51 *et seq.*) (2001). Applicant understands that the making of a false statement on the application or on materials submitted with the application is punishable by criminal penalties pursuant to D.C. Official Code, section 22-2405 *et seq*. (2001).

DRUG-FREE WORK PLACE ACT OF 1988: "PURSUANT TO THE REQUIREMENTS OF THE DRUG-FREE WORKPLACE ACT OF 1988, THE INDIVIDUAL SELECTED TO FILL THIS POSITION WILL, AS A CONDITION OF EMPLOYMENT, BE REQUIRED TO NOTIFY HIS OR HER IMMEDIATE SUPERVISOR, IN WRITING, NO LATER THAN FIVE (5) DAYS AFTER CONVICTION OF OR A PLEA OF GUILTY TO A VIOLATION OF ANY CRIMINAL DRUG STATUTE OCCURRING IN THE WORKPLACE."

OFFICIAL JOB OFFERS ARE MADE ONLY BY THE DCRB HUMAN RESOURCES